

CLERK'S OFFICE

A TRUE COPY

Mar 18, 2022

s/ Daryl Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Property at 214 E Florida Street, Unit 212,
Milwaukee, WI, more fully described in Attachment A.

Case No. 22 MJ 46

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. Sections 371, 922 (g)(1), 922(o) and 1343	Conspiracy, felon in possession of a firearm, illegal possession of a machine gun, and wire fraud.

The application is based on these facts:
See Attached Affidavit

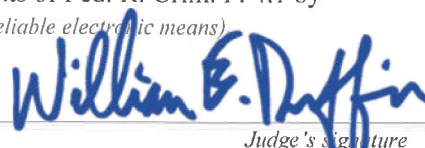
- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Kyle Veloz, FBI Task Force Officer

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ *(specify reliable electronic means)*Date: 3/18/2022City and state: Milwaukee, WI


Judge's signature

Honorable Williams E Duffin, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Kyle Veloz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 214 E Florida Street #212, Milwaukee, Wisconsin, 53204, hereinafter “PREMISES,” further described in Attachment A, for the things described in Attachment B.

2. I have been employed with the Milwaukee Police Department as a full time sworn police officer since June 2018. I am currently assigned as a task force officer (TFO) to the Milwaukee Area Safe Streets Task Force (MASSTF) and the Federal Bureau of Investigation (FBI) Milwaukee Field Office. In April 2021, I was officially sworn in as a federal task force officer to work with the FBI’s gang task force, which provides me with the authorization to present sworn affidavits in support of federal search warrant applications. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

3. I have received training and have experience in the area of controlled substances investigations, money laundering, financial investigations, and various methods that drug dealers use in an effort to conceal and launder the proceeds of their illicit drug trafficking enterprises. I have participated in numerous investigations involving violations of controlled substances laws to include other violations associated with the trafficking of controlled substance. I have participated in numerous drug investigations utilizing various means of investigation including but not limited

to, a wire investigation, the execution of search warrants, the use of subpoenas, and the use of informants.

4. I have been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. I have participated in criminal investigations, surveillance, search warrants, interviews, and debriefs of arrested subjects. As a result of this training and investigative experience, I have learned how and why violent actors typically conduct various aspects of their criminal activities.

5. The facts in this affidavit come from my personal observations, my training and experience, my review of documents, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Since February 2021, the ATF, Milwaukee Police Department (MPD), Federal Bureau of Investigation (FBI), and Drug Enforcement Administration (DEA) have been investigating identified members of the “Wild 100’s”, a violent street gang in Milwaukee, also known as the “Shark Gang”, including Byron J CLAYPOOL Jr (B/M, 07/03/1998), among others, for federal firearms offenses and federal program fraud. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that CLAYPOOL has committed violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C § 922(g)(1) (felon in possession of a firearm), 18 U.S.C. § 922(o) (illegal possession of a machine gun), and 18 U.S.C. § 1343 (wire fraud).

PROBABLE CAUSE

7. CLAYPOOL has emerged as a suspect based upon his connections to the “Wild 100s” street gang. CLAYPOOL has been identified as a Wild 100 member via multiple MPD

reports, multiple sources of information, and an ATF confidential source. Agents have additionally observed CLAYPOOL photographed with several previously identified Wild 100 members. These individuals exclusively claim affiliation with the gang and do not represent other entities in Milwaukee. CLAYPOOL has allegedly been engaged in multiple instances of COVID-19 fraud. In fact, CLAYPOOL has been observed on his own publicly viewable social media profiles (Instagram: “bracks0216”, “doit4_ab” & “longliveab0216” which are the same account) posting several pictures of large amounts of cash, firearms, jewelry, and other items of value.

8. I know the Instagram account “longliveab0216” to be owned and operated by CLAYPOOL. I analyzed Instagram messages between Instagram account “goldhuncho”, who I know to be confirmed Wild 100’s member Chazz D. WHITE (B/M, 11/14/1990), and CLAYPOOL following the receipt of CLAYPOOL’s Instagram return. On March 20, 2021 WHITE stated, “Send yo info a pic of yo ID Nd ssn email phone num.” CLAYPOOL responded with a photograph of his Wisconsin Identification Card. CLAYPOOL went on to provide the email address of “Byronclaypool0216@gmail.com.” CLAYPOOL later provided the social security number “391-19-2765.”



Photo ID

2500134600295573

Author bracks0216 (Instagram: 44533311772)
Sent 2021-03-20 19:53:23 UTC
Body Byronclaypool0216@gmail.com

Author goldhuncho (Instagram: 31578210968)
Sent 2021-03-20 20:21:46 UTC
Body 10k ill bro u gotta bank account rite

Author goldhuncho (Instagram: 31578210968)
Sent 2021-03-20 20:22:00 UTC
Body Somebody doin it fo me

Author bracks0216 (Instagram: 44533311772)
Sent 2021-03-20 20:22:45 UTC
Body Yea a chime

Author goldhuncho (Instagram: 31578210968)
Sent 2021-03-20 20:23:06 UTC
Body Ok I think it a work send ssn

Author bracks0216 (Instagram: 44533311772)
Sent 2021-03-20 20:25:40 UTC
Body 391-19-2765

9. Following the receipt of CLAYPOOL's Instagram return I discovered that there were three registered email addresses associated to CLAYPOOL's Instagram account; byronclaypool1@gmail.com, byronclaypool84@gmail.com, and byronclaypool0216@gmail.com To "register" an address, Instagram requires confirmation by the account holder, CLAYPOOL in this case.

Service Instagram
Target 44533311772
Account Identifier longliveab0216
Account Type InstagramUser
Generated 2021-10-26 21:16:56 UTC
Date Range 2020-01-01 00:00:00 UTC to 2021-09-20 23:59:59 UTC

Ncmec Reports NCMEC Cybertips: NCMEC cybertip reports associated to the account of the sender.
Definition CyberTip ID: Unique identifier associated with the cybertip.
 Time: Date and time the NCMEC cybertip was sent.
 Responsible Id: Identification number of the sender's Facebook account associated with the NCMEC cybertip report.
 Media uploaded in this cybertip: Media associated with the cybertip.
 Id: Unique identifier associated with the media.
 Upload Time: Date and time account holder uploaded the content.
 Ncmec File Id: NCMEC Identifier associated with the cybertip.
 Recipients: The account holder that received the content.

NCMEC No responsive records located
CyberTip Numbers

Name Name: Name provided by the account holder.
Definition First: First name provided by the account holder.
 Middle: Middle name provided by the account holder.
 Last: Last name provided by the account holder.

Name **First** Bee Humble

Emails Registered Email Addresses: Displays a list of registered email addresses. To "register" an address, it requires confirmation by the account holder.

Registered byronclaypool1@gmail.com
Email byronclaypool84@gmail.com
Addresses byronclaypool0216@gmail.com

Vanity Vanity: Username associated with the account.
Definition

Vanity Name longliveab0216

Vanity Changes Vanity Changes: Vanity changes associated with the account.
Definition New Vanity: New vanity selected.
 Old Vanity: Old vanity selected.

Vanity Changes **Old Vanity** bracks0216
New Vanity longliveab0216

Registration Date Definition Registration Date: Date and time of account creation.

Registration Date 2020-11-30 01:43:45 UTC

Registration Ip Definition IP address associated with account creation.

Registration Ip 2603:6000:aa05:600:6831:4d0c:c84c:ebf4

Account End Date Definition Account End Date: Displays the status of the account at the time the records were generated.
Time: Date and time the account was closed.
Reason: The account was closed (deactivated, disabled, deleted).

Account Closure Date **Account Still Active** true

Phone Numbers Definition Phone numbers: Phone number(s) provided by the account holder. "Verified" indicates the account holder responded to a text sent to the listed phone number.

Phone Numbers +14148997570 Verified

11. I analyzed Instagram messages between Instagram account “mr_bounceback100”, who I know to be confirmed Wild 100’s member Ramon E. SAVGE (B/M, 06/13/1995), and CLAYPOOL following the receipt of CLAYPOOL’s Instagram return. On September 20, 2021 CLAYPOOL stated, “Call me right now I’m tryna do sumn 4148997570.”

Body

On lo I gotta thousand dollas to my name Byron dis punk ass bitch
ran off w every dolla cuz I'm fucked up n u got a what

Author mr__bounceback100 (Instagram: 8175427650)

Sent 2021-09-20 23:30:29 UTC

Body Wads unlocked

Author longliveab0216 (Instagram: 44533311772)

Sent 2021-09-20 23:30:57 UTC

Body Call me right now I'm tryna do sumn 4148997570

12. It should be noted that CLAYPOOL is a convicted felon related to State of Wisconsin Circuit Court number 2017CG000189 for 2nd Degree Reckless Injury 940.23(2)(a). Due to the aforementioned felony conviction CLAYPOOL is prohibited from firearm possession.

13. I analyzed Instagram messages between Michael M. ANDERSON (B/M, 04/24/1997), who is a confirmed Wild 100's member, and CLAYPOOL following the receipt of ANDERSON's Instagram search warrant return. On March 3, 2021 CLAYPOOL stated, "Bro call me 414-899-7570 I'll cheese you just to let me hold it down until like 2 weeks when I go to store with my big cuz and grab nice glizzy. I been taking it easy long enough I'm tryna get out here. Full fledged now but I can't with out no smack. My bitch got Ls and shit. I don't really fw niggas so you ion gotta worry bout NO GOOFY shit. On AB." I am aware that the term "cheese" can refer to money or cash. I am aware that the terms "glizzy" and "smack" can refer to Glockes or other firearms. I am aware that the term "Ls" can refer to a Concealed Carry Weapon (CCW) permit. I interpreted this conversation as CLAYPOOL essentially renting a firearm from ANDERSON for two weeks until CLAYPOOL's cousin was able to buy a firearm for him. CLAYPOOL offered ANDERSON money in exchange for the firearm and stated that his girlfriend has a CCW permit.

Author

longliveab0216 (Instagram: 44533311772)

Sent 2021-03-13 19:46:17 UTC**Body** Ina mil? Don't forget about me bro**Author** longliveab0216 (Instagram: 44533311772)**Sent** 2021-03-13 23:17:21 UTC**Body** Bro call me 414-899-7570 I'll cheese you just to let me hold it down until like 2 weeks when I go to store with my big cuz and grab nice glizzy. I been taking it easy long enough I'm tryna get out here. Full fledge now but I can't with out no smack. My bitch got Ls and shit. I don't really fw niggas so you ion gotta worry bout NO GOOFY shit. On AB

14. On May 20, 2021 CLAYPOOL sent ANDERSON a message which stated, "Wya nigga I pick up new glock today." CLAYPOOL informed ANDERSON that he acquired a Glock firearm.

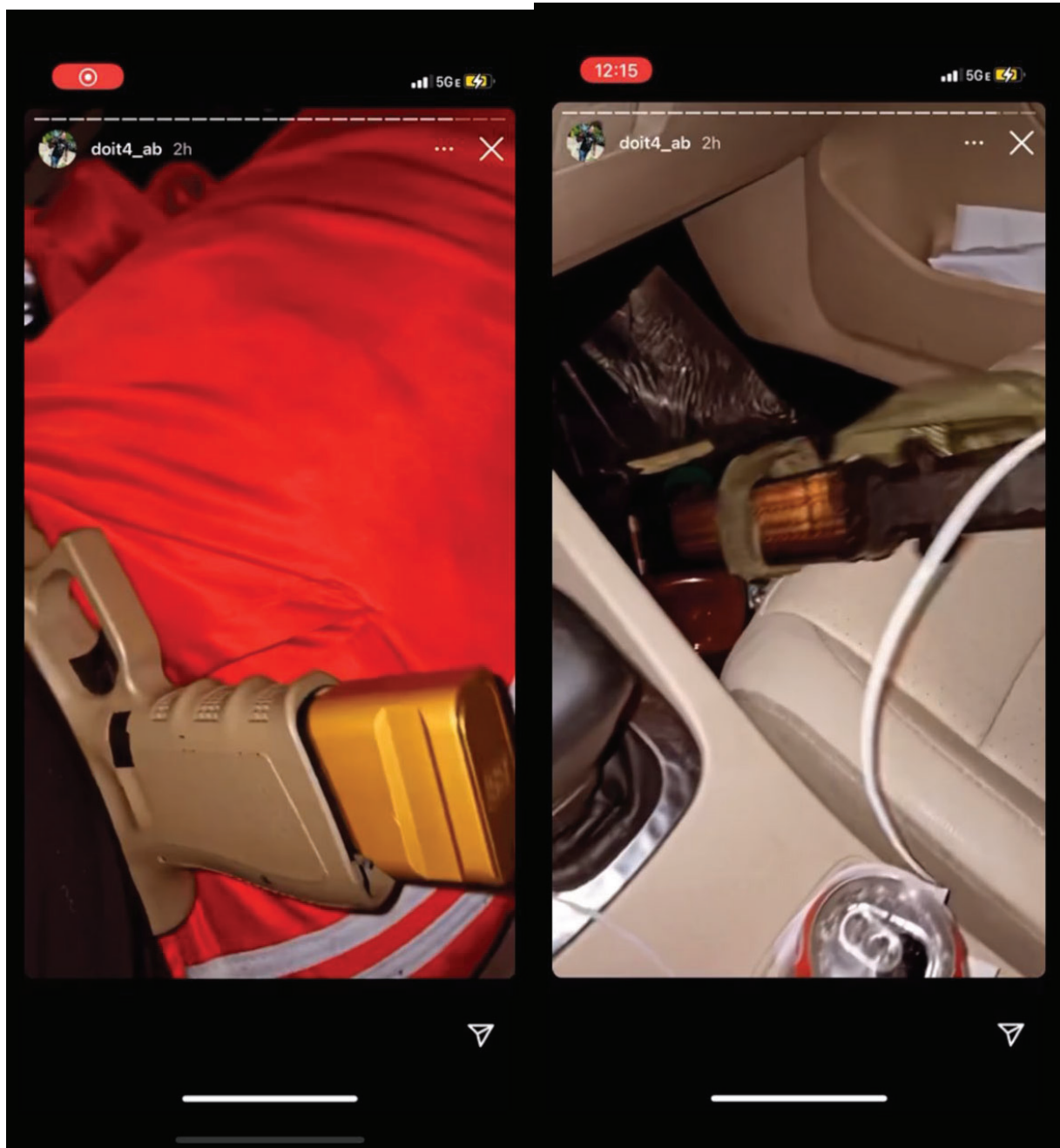
Body

How much 15s go for now

Author longliveab0216 (Instagram: 44533311772)**Sent** 2021-05-20 16:17:31 UTC**Body** \$35 but u can get \$40 they'll pay**Author** longliveab0216 (Instagram: 44533311772)**Sent** 2021-05-20 16:17:51 UTC**Body** Wya nigga I pick up new glock today

15. On December 11, 2021 at approximately 10:00 PM CLAYPOOL posted a video to his Instagram story. The video depicts a tan Glock firearm with a gold extended magazine protruding from the magazine well resting on CLAYPOOL's lap. In the video CLAYPOOL is wearing red track pants with two white stripes going from his waist down. It should be noted that in the video you can see that CLAYPOOL does not have a left leg. CLAYPOOL lost his left leg in a car accident in 2017. The video continues and CLAYPOOL manipulates a top loading AR style pistol with a green casing catchers attached to the lower, which is located in the front floor board of the vehicle. Bullets can be seen in the magazine due to the magazine being transparent.

During the video CLAYPOOL flips the camera over so his face can be seen while he is pointing the Glock at the camera. CLAYPOOL is wearing a pair of Cartier Style glasses with custom lenses.





Fraud Related to COVID-19 Relief Programs

16. Pursuant to legal process served on Google, they returned subscriber, IP data, and

email header information. The subscriber name (Google Account ID: 239301598950) was listed as Byron CLAYPOOL with a date of birth of July 3, 1998. According to a Google document, the listed email address on the aforementioned Google account for CLAYPOOL is byronclaypool658@gmail.com. According to the Google document, the listed phone number on the aforementioned Google account for CLAYPOOL is (414) 899-7570. It should be noted that the phone number associated the Google account is the same phone number verified on CLAYPOOL's Instagram and the same phone number that CLAYPOOL provided to various other Instagram users throughout his Instagram warrant return.

17. Pursuant to the legal process served on Google, sixty-six (66) separate email accounts were linked to the email address mentioned in paragraph fifteen (15). The 66 email addresses were linked by Cookies. Cookies are small text files sent by the website you're visiting to the computer or device you're using. If accepted, these cookies are stored on the web browser of your device. Cookies can then track and collect data from your browser, sending that data back to the website owner.¹

18. Pursuant to the legal process served on Google, nineteen (19) separate email addresses were linked to the phone number mentioned in paragraph fifteen (15).

19. I have learned from multiple sources, including posts by Wild 100's members on social media, that the Wild 100's are engaged in multiple schemes to defraud unemployment insurance and COVID-19 relief programs. For example, I have seen posts and videos on social media where Wild 100's members use the California EDD system to file fraudulent unemployment claims in the names of third parties. They access the site, and file a claim utilizing someone's date of birth, social security number, and phone number. Most individuals split the profits with the

¹ Source: Norton Security, available at <https://us.norton.com/internetsecurity-privacy-should-i-accept-cookies.html>

person supplying their identity for the claim. The CARES Act established a new program—PUA—to provide unemployment benefits during the COVID-19 pandemic to people who do not qualify for regular unemployment insurance benefits including business owners, self-employed workers, independent contractors, and those with a limited work history who are out of business or have significantly reduced their services as a direct result of the pandemic. Unemployment insurance benefits provided under the PUA program are sometimes referred to as PUA benefits. Each state's unemployment insurance office is responsible for distributing these benefits if available in that state.

20. In many states, PUA is distributed in the form of debit cards that are mailed directly to the beneficiary. The beneficiary may then use the debit card to withdraw the PUA funds from an ATM. Once the claim is approved, the individual committing the fraud will log into EDD and change the mailing address for the loaded debit card to be sent to a Milwaukee address. The individual will then withdraw the money from these loaded debit cards from an ATM and split the profits with the individual for whom they are filing the false claim.

21. I analyzed Instagram messages between Michael M. ANDERSON (B/M, 04/24/1997), who is a confirmed Wild 100's member, and CLAYPOOL following the receipt of ANDERSON's Instagram search warrant return. The two discussed different schemes to earn money. On June 20, 2021, CLAYPOOL shared two screenshots of the California Employment Development Department (EDD) website which depicts two separate accounts with the total amounts paid as \$12,141.00 and \$19,350.00 in insurance benefits between the dates of June 17, 2021 to June 19, 2021.

[Search](#)[Reset](#)

ance benefits issued between 06/17/2021 and 06/19/2021: \$12,141.00

<u>Payment Issued</u>	<u>Payment ID</u>	<u>Payment Status</u>	<u>View</u>
\$366.00	11080957	Paid	Details
\$966.00	11080958	Paid	Details
\$966.00	11080961	Paid	Details
\$666.00	11112288	Paid	Details
\$966.00	11112289	Paid	Details
\$966.00	11112292	Paid	Details
\$483.00	11017640	Paid	Details
\$966.00	11017643	Paid	Details
\$966.00	11017642	Paid	Details
\$966.00	11017638	Paid	Details
\$966.00	11017639	Paid	Details
\$966.00	11049086	Paid	Details
\$966.00	11049090	Paid	Details
\$966.00	11049089	Paid	Details

[Return](#)[Contact EDD](#)[Conditions of Use](#)[Privacy Policy](#)[Accessibility](#)

Payment History

Click here to view information about payments issued during the selected date range.

From Date: (MM/DD/YYYY) *To Date: (MM/DD/YYYY)

Search

Reset

Payment History

Insurance benefits issued between 06/17/2021 and 06/19/2021: \$19,350.00

Payment Issued	Payment ID	Payment Status	View
\$750.00	11061925	Paid	Details
\$1,500.00	11061927	Paid	Details
\$1,500.00	11061929	Paid	Details
\$1,500.00	11061928	Paid	Details
\$900.00	11124124	Paid	Details
\$1,200.00	11124125	Paid	Details
\$1,500.00	11124126	Paid	Details
\$1,500.00	11124130	Paid	Details
\$1,500.00	11124131	Paid	Details
\$1,500.00	11030989	Paid	Details
\$1,500.00	11030993	Paid	Details
\$1,500.00	11092753	Paid	Details
\$1,500.00	11092756	Paid	Details
\$1,500.00	11092759	Paid	Details

Return

[Top](#)

[Contact EDD](#)

[Conditions of Use](#)

[Privacy Policy](#)

[Accessibility](#)

22. On July 1, 2021, CLAYPOOL stated, “I wanted to come down there but I’m swiping heard [sic] the cards lick if you try to swipe OT.” I’m aware that the term “swiping cards” can refer to committing identify theft and stealing individuals benefits that are sent to them via pre-paid debit cards.

Body
Video call ended

Call Record **Missed** false
 Duration 208842

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-06-20 20:17:54 UTC
Body Wats yo number

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-06-23 04:35:25 UTC
Body Aye bro

Author ikey4blk (Instagram: 44261471194)
Sent 2021-06-23 04:38:20 UTC
Body Wtw

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-06-23 04:56:25 UTC
Body Call me 414-899-7570 I been tryna holla at you bout some real shit

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-06-26 05:57:20 UTC
Body Aye put me up on some beasty designer I should wear on my bday bro

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-06-29 13:37:53 UTC
Body []
Share **Date Created** Unknown

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-06-30 15:46:31 UTC
Body []
Share **Date Created** Unknown
 Url <https://instagram.com/stories/ikey4blk/2607571329008732684>

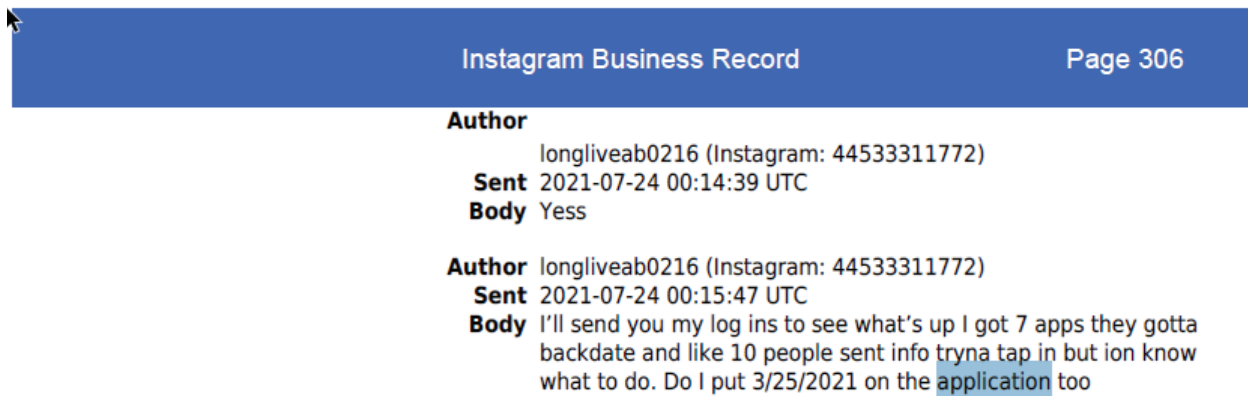
Author longliveab0216 (Instagram: 44533311772)
Sent 2021-07-01 04:53:30 UTC
Body U in town ? Yk my bday in two days bitch

Author ikey4blk (Instagram: 44261471194)
Sent 2021-07-01 05:01:04 UTC
Body Hell naw I'm n Texas

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-07-01 05:39:00 UTC
Body I wanted to come down there but I'm swiping heard the cards lick if you try to swipe OT

23. I analyzed Instagram messages between Instagram user “bogaty_espiritu” and CLAYPOOL following the receipt of CLAYPOOL’s Instagram search warrant return. On July

24, 2021, CLAYPOOL stated, “I’ll send you my log ins to see what’s up I got 7 apps they gotta backdate and like 10 people sent info tryna tap in but ion know what to do. Do I put 3/25/2021 on the application too.” I am aware that the term “apps” can refer to EDD applications.



24. I analyzed Instagram messages between Instagram user “_mevsmi” and CLAYPOOL following the receipt of CLAYPOOL’s Instagram search warrant return. On August 16, 2021 CLAYPOOL stated, “Who tryna make 20k you just need 3 forms of IDENTIFICATION, I just want 5-7k.” I am aware that in order to apply for unemployment with the California EDD, three forms of identification are needed. Subjects who are seeking new “clients” often send out messages similar to the aforementioned message sent by CLAYPOOL.

Author __mevsmi (Instagram: 15530283659)
Sent 2021-08-13 21:05:23 UTC
Body Video call ended
Call Record **Missed** false
Duration 57576

Author __mevsmi (Instagram: 15530283659)
Sent 2021-08-14 00:46:49 UTC
Body Message unavailable
Share **Date Created** Unknown

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-08-14 00:47:24 UTC
Body You sent an attachment.
Share **Date Created** Unknown
Url <https://instagram.com/stories/longliveab0216/2639744037808810924>

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-08-15 04:09:17 UTC
Body [REDACTED]
Share **Date Created** Unknown

Author __mevsmi (Instagram: 15530283659)
Sent 2021-08-16 19:35:39 UTC
Body Send me that stuff you need for edd so I can post on my pages

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-08-16 20:05:25 UTC
Body You was posed to send me yo page info

Author __mevsmi (Instagram: 15530283659)
Sent 2021-08-16 20:06:06 UTC
Body I don't know my stuff I have to figure out my password

Author longliveab0216 (Instagram: 44533311772)
Sent 2021-08-16 20:09:11 UTC
Body Who tryna make 20k you just need 3 forms of IDENTIFICATION, I just want 5-7k

The Premises to be Searched

25. According to public records checks with the Wisconsin Department of Transportation, as of June 28, 2021, CLAYPOOL's address on file is listed as 214 E Florida Street #212, Milwaukee, Wisconsin, 53204, the PREMISES. According to the Department of Corrections, CLAYPOOL's listed address is 214 E Florida Street, Milwaukee, Wisconsin, 53204, the PREMISES.

26. On February 14, 2022 I observed photos uploaded to CLAYPOOL's Instagram account. The photo depicts CLAYPOOL sitting on the kitchen counter. In the photo CLAYPOOL is wearing Cartier glasses with custom lenses and a white puffy coat with Sherpa lining and red zipper strings. The counter tops are white in color, the cabinets are black with silver handles, the refrigerator is black with a stainless steel door, and the wall appears to be 2"x4" pieces of wood cut to different lengths used as a backsplash. I reviewed photos from the Maxwell Lofts website (maxwellmilwaukee.com) and determined that the cabinets, counter tops, refrigerator, and backsplash match those of the photograph uploaded by CLAYPOOL. According to the Maxwell Lofts website, Maxwell Lofts are located at 214 E Florida Street, Milwaukee, WI 53204.





27. On October 6, 2021 at 11:35 AM TFO Richard KLARKOWSKI and I conducted an interview of Jaquan A WRIGHT (B/M, 08/08/1999), a confirmed Wild 100's member². During the interview WRIGHT provided information on CLAYPOOL. WRIGHT stated that an associate of his known as "B Racks", which is an alias for CLAYPOOL, was in possession of a "Ghost Glock" with an "internal switch" along with other firearms. I am aware that a "Ghost Glock" is a Glock style handgun that does not have any serial numbers, which essentially makes the firearm untraceable. I am aware that the term "switch" can refer to an auto-sear. I am aware that auto-sears are items installed on the backplate of Glock brand firearms and these devices illegally convert the firearm from semi-automatic to fully automatic. I am aware that auto-sears are considered a machine gun by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) definition and thus making them illegal to possess under both federal and Wisconsin State Statute 941.26(1g)(a) which states "No person may sell, possess, use, or transport any machine gun or other full automatic firearm." *See also* 18 U.S.C. § 922(o), and 26 U.S.C. 5845(b). During the interview, WRIGHT provided TFO KLARKOWSKI and I with CLAYPOOL'S residence. Using google maps, WRIGHT pointed out the Maxwell Lofts located at 214 E Florida Street as the apartment building where CLAYPOOL resides.

28. I analyzed Instagram messages between Instagram user "marc0bricks" and CLAYPOOL following the receipt of CLAYPOOL's Instagram search warrant return. On

² WRIGHT's prior convictions include : Receiving Stolen Property (>\$2500-\$5000) [Modifiers: PTAC, as a Party to a Crime], a class I felony, Wisconsin Statutes 943.34(1)(bf), Possess Drug Paraphernalia [Modifiers: PTAC, as a Party to a Crime], an unclassified misdemeanor, Wisconsin Statutes 961.573(1), Battery, a class A misdemeanor, Wisconsin Statutes 940.19(1), Operate Vehicle w/o Consent-Passenger [Modifiers: PTAC, as a Party to a Crime], a class A misdemeanor, Wisconsin Statutes 943.23(4m), Possess Firearm-Convicted of a Felony, a class G felony, Wisconsin Statutes 941.29(1m)(a), Bail Jumping-Felony, a class H felony, Wisconsin Statutes 946.49(1)(b), Operating While Revoked (Rev due to alc/contr subst/refusal), an unclassified misdemeanor, Wisconsin Statutes 343.44(1)(b), Bail Jumping-Felony, a class H felony, Wisconsin Statutes 946.49(1)(b). WRIGHT provided information in hopes of having his probation hold lifted. WRIGHT was informed that PO KLARKOWSKI and I could not help him with his probation hold.

September 8, 2021 “marc0brickz” asked, “You got a good address?” CLAYPOOL replied, “Yup” and later stated, “214 E Florida St Milwaukee, WI 53204.”



TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:
- IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
 - Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- d. SMS: Short Message Service (or simply “SMS”) is used to send text messages to mobile phones. The messages can typically be up to 160 characters in length, though some services use 5-bit mode, which supports 224 characters.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be

recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

32. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the

purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and

malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described

herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence

or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

- f. I know that when an individual uses a computer to submit fraudulent applications for benefits, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

33. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing

evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a

later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

35. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

Property to be searched

The property to be searched is 214 E Florida Street, Milwaukee, WI, the “PREMISES”, which is apartment unit number 212 of a red brick apartment style building, which bears white numerals reading “214” on the front of the building along with the name “MAXWELL” on the front of the building in white letters. A picture of the Subject Residence follows.





ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C § 922(g)(1) (felon in possession of a firearm), 18 U.S.C. § 922(o) (illegal possession of a machine gun), and 18 U.S.C. § 1343 (wire fraud) involving Byron J CLAYPOOL Jr, DOB: 07/03/1998:
 - a. Firearms and/or ammunition;
 - b. Records and information relating to the illegal possession of firearms, including machine guns as defined by 26 U.S.C. 5845(b);
 - c. Records and information relating to a conspiracy to defraud the government;
 - d. Records and information relating to an access of US currency fraudulently obtained using another individual's identity;
 - e. Records and information relating to COVID-19 relief;
 - f. Records and information relating utility bills, writings, cell phones, computers, receipts, and/or other documentary evidence establishing who is in control of the premises;
 - g. Records and information relating to the identity or location of the suspects.
2. Computers or storage media used to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;

- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may

include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.